

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09305661 A**

(43) Date of publication of application: 28 . 11 . 97

(51) Int. Cl. **G06F 17/60**  
**G06F 15/00**  
**G09C 1/00**  
**G09C 1/00**  
**H04L 9/32**

(21) Application number: **08116012**

(22) Date of filing: **10 . 05 . 96**

(71) Applicant: **HITACHI LTD**

(72) Inventor: **KAWAZURE YOSHIAKI**  
**CHIBA HIROYUKI**

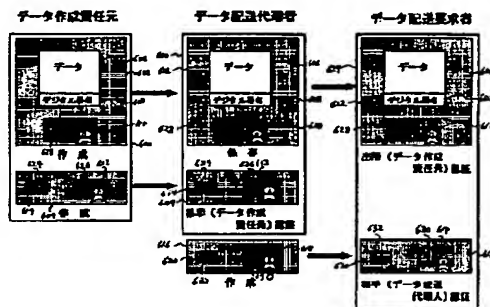
(54) **SOURCE AUTHENTICATING METHOD**

(57) Abstract:

**PROBLEM TO BE SOLVED:** To provide a source authenticating method for making the generation responsible source of transmission data clear.

**SOLUTION:** A means for mutually authenticating two parties actually executing communication is buried in an electronic envelope part (604 and 616) and a means for authenticating a data generation responsible person by a data delivery requesting person is buried in a ciphering data part (602) so that a data delivery agent authenticates the data generation responsible source by the electronic envelope 604 part. The electronic envelope is re-generated so as to permit the data delivery requesting person to authenticate the data delivery agent (616) and delivered to the data delivery requesting person so that the data delivery agent is authenticated and the data source is authenticated by a cipher or data 622 part.

COPYRIGHT: (C)1997,JPO



(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-305661

(43) 公開日 平成9年(1997)11月28日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 17/60			G 0 6 F 15/21	Z
15/00	3 3 0		15/00	3 3 0 A
G 0 9 C 1/00	6 4 0	7259-5 J	G 0 9 C 1/00	6 4 0 A
		7259-5 J		6 4 0 B
	6 6 0	7259-5 J		6 6 0 E

審査請求 未請求 請求項の数 1 O L (全 10 頁) 最終頁に続く

(21) 出願番号 特願平8-116012

(22) 出願日 平成8年(1996)5月10日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 川連 嘉晃

神奈川県横浜市都筑区加賀原二丁目2番株

式会社日立製作所ビジネスシステム開発セ  
ンタ内

(72) 発明者 千葉 寛之

神奈川県横浜市都筑区加賀原二丁目2番株

式会社日立製作所ビジネスシステム開発セ  
ンタ内

(74) 代理人 弁理士 小川 勝男

## (54) 【発明の名称】 出所認証方法

## (57) 【要約】

【課題】本発明は送付データの作成責任元を明確化する出所認証方法を提供することにある。

【解決手段】実際に通信する2者間がお互いを認証する手段を電子封筒部分(604、616)に、データ配送要求者がデータ作成責任者を認証する手段を暗号化データ部分に埋め込む(602)ことにより、データ配送代理人は、電子封筒604部分でデータ作成責任元を認証することができ、また、電子封筒を、データ配送要求者が、データ配送代理人を認証できるように再作成して(616)、データ配送要求者に配送することにより、データ配送代理人を認証することができ、また、暗号化データ622部分により、データの出所認証をする事ができる。

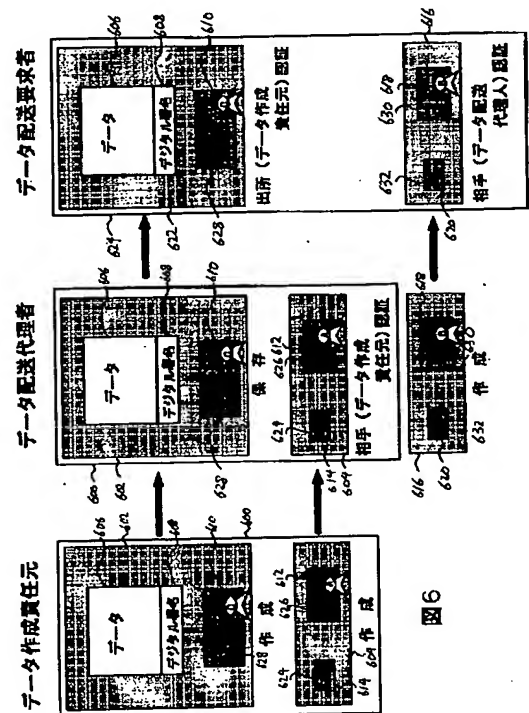


図6

**【特許請求の範囲】**

**【請求項1】** データを複数者間を経由してデータの発元と、發送依頼先で安全な通信で送付する場合に、実際に通信する2者間がお互いを認証する手段と、データ最終受取者が發送開始者を認証する手段を分割することを特徴とする出所認証方法。

**【発明の詳細な説明】****【0001】**

**【発明の属する技術分野】** 本発明は共通鍵暗号方式と公開鍵暗号方式を用いた電子商取引に関し、特に配布データの作成元／責任元を明確にすることができる、データの出所認証方法に関する。

**【0002】**

**【従来の技術】** 商取引をネットワーク、特にインターネットで行う電子商取引においては、買い手は世界中のインターネット上にある仮想店舗にアクセスし、多種多様な商品を購入することができる。また、購入できる商品は、洋服等の形のある「品物」だけでなく、ネットワークを通じて配送できる、ソフトウェア等の形のない「データ」をも含まれる。

**【0003】** しかし、インターネットを用いて電子商取引を行う場合にはソフトウェア等のデータのやり取りの安全性が問題となる。つまり、データの漏洩や、改竄、配送元のなりすまし等の犯罪を比較的容易に行うことができるからである。

**【0004】** このような問題に対して、共通鍵暗号方式や、公開鍵暗号方式といった暗号化方式を使って、安全なデータのやり取りを実現することが一般的である。ここで、共通鍵暗号方式とは、暗号化する時に使用する鍵と復号化する時に使用する鍵が同じである暗号方式であり、暗・復号速度が高速なので、大量のデータを暗号化するのに適している。これに対して公開鍵暗号方式とは、他者に見せない鍵(秘密鍵)と、それに対応する、他者に公開する鍵(公開鍵)がペアになっていて、一方の鍵を使用して作られた暗号文は、ペアのもう一方の鍵を使用しなければ復号化できない方式であり、不特定多数の人と通信することに適している。

**【0005】** また、証明書発行局という、信頼できる第3者機関が発行した電子的な証明書(以下、証明書)を使用することにより、取引相手の身元を証明し、通信元のなりすましを防止する方法が提案されている。証明書発行局は一つとは限らず、通信先、通信元の双方が、信頼できる同じ証明書発行局からの証明書を持っていれば相手の認証が可能である。

**【0006】** 以下、証明書発行局の証明書を用いた、データ作成責任元(以下、作成責任元)とデータ配送要求者(以下、配送要求者)間での安全なデータのやり取りを行う場合の手順を説明する。

**【0007】** まず、配送要求者は証明書をネットワークを通じて作成責任元に送付する。証明書の中には、認証

対象者の公開鍵と、それを認証した証明書発行局のデータなどが暗号化されて入っており、認証は双方の電子的な証明書の中に入っている証明書発行局のデータを突き合わせる事で行う。

**【0008】** 作成責任元は、配送要求者から送られた証明書を、同じ証明書発行局から発行された、証明書を用いて相手認証する。もし認証できたならば、作成責任元は要求されたデータと、データを元に生成したデジタル署名、デジタル署名を復号化する公開鍵の含まれた電子的な証明書を新たに生成した共通鍵で暗号化する。ここで、デジタル署名は、データの改竄を防止する役割をはたす。

**【0009】** 次に、生成した共通鍵を相手に送付しないと復号化できないため、電子封筒に包み込んで送付する。ここで、電子封筒とは、相手先から送付された証明書内の公開鍵で、共通鍵を暗号化したものをさし、送付データの漏洩を防ぐ役割を果たす。そして、電子封筒と、データ等を暗号化したものといっしょに配送要求者へ送付する。

**【0010】** 配送要求者は、送られてきた電子封筒を配送要求者の秘密鍵で復号し、共通鍵を取り出し、暗号化されたデータを復号する。復号化できたならば、復号化により取り出された作成責任元の証明書と、デジタル署名を用いて、相手認証と、データが改竄されていないかを確認する。この一連のプロセスにより、2者間での安全なデータの受渡しを実現することができ、2者間の出所認証も実現される。

**【0011】** 配送要求者と作成責任元の間にデータ配送代行者(以下、配送代行者)が存在し、データ配送代行者経由でデータのやり取りをする場合には、配送要求者の証明書を配送代行者経由で作成責任元に送付し、送付者が証明書内に入っている公開鍵で電子封筒を作成することにより、配送代行者経由で3者間での安全なデータの受渡しを実現し、配送要求者は、作成責任元を認証することができる。つまり、作成責任元の出所認証を実現している。

**【0012】** しかし、配送要求者の証明書を配送代行者を通して作成責任元に配送し、暗号化する方式では、通信コストが膨大となる。なぜなら、ソフトウェア等のファイルの大きさは膨大になるので、配送代行者はソフトウェアの要求のたびに、データ配送者との間の通信コストがかかり、また、オンライン通信の場合、配送要求者はデータ配送代行者との間の通信コストのほかに、データ配送代行者とデータ配送者間の通信コストもかかってしまい、非常に非効率である。

**【0013】** このような問題に対して、従来は、前述の2者間の安全な配送方式を用いて、配送代行者経由での配送を3者間の非同期な場合と位置づけ、まず、作成責任元と配送代行者間で安全なデータのやり取りを行ない、データを配送代行者に保管しておき、配送要求者が

配送代行者に発送依頼をし、配送要求者と配送代行者間で安全にデータのやり取りをすることによってこの問題を解決している。

#### 【0014】

【発明が解決しようとする課題】かかる従来の方法においては、次のような問題がある。

【0015】すなわち、前述の2者間の安全な配送方式を用いて、配送代行者と作成責任者との間の通信と、配送代行者と配送要求者との間の通信に分割し、データを配送代理人のディスクに蓄積させる方法では、配送代理人にデータを改竄される可能性がある。なぜなら、証明書を検証し、デジタル署名にかけられている暗号をはずすことにより配送代理人は、データ作成責任者を認証するので、データ配送代行者の認証のために作り直すことになってしまう。つまり、配送要求者に届くデータに付いている証明書やデジタル署名は配送代行者のものなので、オリジナルの作成者の人稱を行なうことが出来なくなる。

【0016】本発明の目的は、通信コストを下げるためにデータ配送代行者にデータを保管した場合に、送付データの作成責任元を明確化することができる出所認証方法を提供することにある。

#### 【0017】

【課題を解決するための手段】本発明は、配送代行者を経由したデータ配送の場合の出所認証において、出所認証を行う部分と、二者間通信の相手認証を行う部分を分ける。例えば、デジタル署名と、それを復号化する公開鍵を含んだ証明書で出所認証を行ない、電子封筒内の暗号化された共通鍵とそれを復号化する公開鍵を含んだ証明書をもちいて、二者間通信での相手認証を行う。実際に通信する2者間は、電子封筒部分で、通信先は、通信元を認証することができる。そこが配送代行者などの中継機関ならば、データ、デジタル署名、それを復号化する公開鍵を含んだ証明書を保管しておく。配送代行者から配送要求者へは、配送要求者が配送代行者を認証できるように、電子封筒を新たに作って配送する。このために、配送要求者は、電子封筒部分で配送代行者を認証し、デジタル署名と、それを復号化する公開鍵を含んだ証明書によって、作成責任者を認証、つまり出所認証を行うことができる。

#### 【0018】

【発明の実施の形態】以下、本発明の実施の形態を詳細に説明する。

【0019】図1は本発明における、配送代理人を介したデータ配送のシステム構成を示す構成図である。本実施例では、データの作成責任元と、そのデータを要求している者の間に、データの配送の代行者が存在する。また、本実施例において、配送代行者は1つとしたが、複数者存在してもかまわない。

【0020】図1において、100は実際にデータを作

成した、データの出所を保証する、作成責任元のデータ配送サーバである。102はメインメモリ、104はディスク装置であって、ディスク装置104の中には、データ(160)、データのデジタル署名(162)、データの出所認証に用いられる証明書と配送代理人との認証を行うための証明書(164)、証明書に対応した公開鍵・秘密鍵(166)等が格納されている。112はディスプレイ、114は入力装置であり、データの作成などに用いる。108は通信装置であり、ネットワーク回線110を介して配送代理人の配送クライアント120との通信を行う。106はこれらすべてを制御する制御装置である。

【0021】120はデータ作成責任元から配送された暗号化データ、電子封筒の復号、相手認証、データ保管等を行なうための、作成責任元の配送サーバ100に対する、配送代行者のデータ配送クライアントであり、かつ、配送要求者にデータを配送するためのデータ配送サーバでもある。122はメインメモリ、124は作成責任元の配送サーバから配送されたデータ(160)、デジタル署名(162)、証明書(164)を保管するディスク装置2であり、126は相手認証を行うための証明書や配送要求者が配送代行者を認証するための証明書(168)、各証明書に対応した秘密鍵・公開鍵(170)等が格納されているディスク装置である。入力装置134、ディスプレイ136は作成責任元サーバ100に対する指示操作と相手認証確認に用いられる。130は通信装置であり、作成責任元との通信に用いるネットワーク回線110、または、配送要求者との通信に用いるネットワーク回線132を通じて通信する。128はこれらすべてを制御する制御装置である。

【0022】140は配送代理人から受け取り、データの出所認証等を行うためのクライアントである。142はメインメモリであり、144は、出所認証を行うための証明書や配送代理人の認証をするための証明書(172)、証明書に対応した秘密鍵・公開鍵(174)等を格納しているディスク装置1である。入力装置146、ディスプレイ148は配送代理サーバに対する指示操作と出所認証確認に用いられる。150はサーバとの通信を行う通信装置であり、152はこれらクライアントの制御を行う制御装置である。

【0023】ここに示した構成は一例であって、もちろんほかの構成もありうる。例えば、データ配送代理人のディスク構成は一つに統合してもかまわない。

【0024】図2は作成責任元でのデータ暗号化プロセスブロック図である。図3はデータ配送代理人での作成責任元との間のデータ復号、相手認証、データ格納プロセスブロック図である。図4はデータ配送代理人の配送要求元データを出す時のデータ暗号化プロセスブロック図である。図5はデータ配送要求者の配送代行者との間のデータ復号、配送元認証、データ出所認証プロセスブ

ロック図である。また、図6は、配送代理人を介したデータ配送における出所認証プロセスの概要図である。

【0025】本実施例においては、証明書発行局は、A(作成責任元と配送代理者を認証)、B(配送代理者と配送要求者を認証)、C(作成責任者と配送要求者を認証)の3つが存在し、証明書を発行していると仮定する。また、証明書内には各々の証明書発行局に認証された公開鍵が含まれていて、各々の認証局に認証された公開鍵はそれぞれ違う公開鍵だと仮定する。つまり、3者は各々2種類の証明書と、2種類の公開鍵・秘密鍵のペアをもっている。以下では、例えば証明書発行局Aが発行した作成責任元の証明書は、「作成責任元の証明書A」と表記し、その証明書に含まれる公開鍵、ならびにそれに対応する秘密鍵は、「作成責任元の公開鍵A/秘密鍵A」と表記する。また、本実施例において、共通鍵については、作成責任元で生成するものと配送代理者が生成するものの2種類が使用される。

【0026】図6において、600は作成責任元からデータ配送代理者への配送メッセージである。メッセージ600は、暗号化データ602と電子封筒604から構成されている。暗号化データ602は、配送対象データ606、配送データのデジタル署名608、作成責任元の公開鍵C(628)を含んだ作成責任元の証明書C(610)が共通鍵624で暗号化されている。ここで、本実施例において、共通鍵暗号方式は特願昭63-103919を用いる。

【0027】電子封筒604は、作成責任元の公開鍵A(626)を含んだ作成責任元の証明書A(612)と、作成責任元の公開鍵(626)で暗号化されている暗号化共通鍵614が、配送代理者の公開鍵で暗号化されている。ここで、本実施例において、公開鍵暗号方式には特公昭59-50068を用いる。

【0028】616は、配送代理者が作成する電子封筒である。電子封筒616は、配送代理者の公開鍵B(630)を含んだ配送代理者の証明書B(618)と、その証明書内の公開鍵(632)で暗号化されている暗号化共通鍵620が、配送要求者の公開鍵で暗号化されている。

【0029】624は、配送代理者から配送要求者への転送メッセージである。メッセージ600は、暗号化データ622と電子封筒616から構成されている。暗号化データ622は、データ606、デジタル署名608、作成責任元の証明書C(610)を、データ配送代理者が新たに生成した、620内の共通鍵626で暗号化されている。

【0030】次に、図2、3、4、5のブロック図、図6の出所認証プロセス概要図に基いた、配送代理人を介したデータ配送時の出所認証法について説明する。

【0031】まず最初に図6を用いて、配送代理人を介したデータ配送における出所認証プロセスの概要を説明

する。

【0032】データ作成責任元は、データ配送要求者が作成責任元を認証できるように暗号化データ602を、また、配送代理者が作成責任元を認証できるように電子封筒604を作成し、配送代理者に配送する。つまり、電子封筒604で作成責任元と配送代理者の間の相手認証を、暗号化データ602で出所認証を行なうことになる。データ配送代理人は、電子封筒604部分で、作成責任元を認証する。認証できたならば、暗号化データ602を614内の共通鍵624で復号して、データ606、デジタル署名608、証明書610を保管する。配送代理者から配送要求者へは、配送要求者が配送代理者を認証できるように、新たに作成した共通鍵632を使って暗号化データ622を生成し、また、電子封筒616を新たに作って配送する。配送要求者は、電子封筒部分616で配送代理者を認証し、暗号化データ622部分で、作成責任元を認証、つまり出所認証を行う。

【0033】次に図2を用いて、作成責任元での配送メッセージ作成プロセスを説明する。

【0034】はじめに配送代理者が作成責任元に対して、データ配送要求のために、配送代理者の証明書Aを配送する。次に、配送データのデジタル署名を作成する。本実施例においては、データをハッシュ関数と呼ばれる特殊な関数により、一定の長さのハッシュ値と呼ばれる値に変換したものを、秘密鍵で暗号化する方式を採用する。ハッシュ値は、一意に定まるので配送元で配送するデジタル署名のハッシュ値と、配送先で配送データをハッシュ化したものを突き合わせる事により、改竄を防止する。

【0035】はじめに、配送対象データをハッシュ関数を用いてハッシュ化し(200)、作成責任元の秘密鍵Cで暗号化し(202)、デジタル署名(608)を作る。この一連のデジタル署名作成プロセスは204に対応する。次に暗号化データを生成するための共通鍵(624)を作成(206)する。この共通鍵(624)を使って、データ(606)、デジタル署名(608)、作成責任元の証明書C(610)を暗号化する(208)。ここまでのプロセス210が、図7の暗号化データ602の生成に対応する。次に、図6の604に対応する電子封筒(604)を作成する。まず、206で生成した共通鍵(624)を作成責任元の秘密鍵Aで暗号化(212)し、その成果物(614)と、作成責任元の証明書A(612)を、218により取り出した、配送代理人の公開鍵Aで暗号化(214)する。この一連の電子封筒生成プロセス(216)により、図6の604部分が生成される。最後に、210、214により生成したメッセージ600をデータ配送代理人に配送する。

【0036】上述の実施例において、作成責任元での配送メッセージ作成プロセスを、配送代理者の証明書が配送された時点から開始する形態を取っているが、これ

は、作成責任元から配送代行者へ配送をする許可を要求し、それを受けて配送代理者が証明書を配送するような形態にしてもよい。

【0037】続いて図3を用いて、データ配送代理人での配送認証処理ならびに配送データ等の格納プロセスを説明する。

【0038】まず、データ作成責任元から受け取った、暗号化データ(602)と電子封筒(604)のうち、電子封筒(604)を、配送代理者の秘密鍵Aで復号し、暗号化共通鍵(614)と、作成責任元の証明書A(612)を取り出す(300)。次に、取り出した証明書(612)と同じ証明書発行局で発行された、データ配送代理人の証明書Aを用いて、配送された証明書が本物かどうかを検証する(302)。検証されたら、作成責任元の証明書A(612)に含まれている公開鍵A(626)を取り出し(304)、306で、共通鍵(624)を取り出す。この、302、304、306のプロセス308により、配送代理人はデータ作成責任元を認証することができる。最後に、共通鍵(624)を用いて暗号化データ(602)を復号化し、データ(606)、デジタル署名(608)、作成責任元の証明書C(610)を取り出し(310)、それらをディスク装置2(124)に格納する(312)。

【0039】上述の実施例において、作成責任元が生成した共通鍵(624)で暗号化データ602を復号化して、データ606、デジタル署名608、作成責任元の証明書C(610)をディスク2(124)に格納する形態をとっているが、復号化せず、暗号化データ602と共通鍵624をディスク装置2(124)に格納する形態を取ってもよい。

【0040】続いて、図4を用いて、データ配送要求者が、データ配送代理人を認証できるような電子封筒の作成ならびに、暗号化データと新たに作成された電子封筒のデータ配送要求者への配送プロセスを説明する。

【0041】はじめに配送代理者が作成責任元に対して、データ配送要求のために、配送要求者の証明書Bを配送する。証明書を受け取った配送代理者は、ディスク装置2(124)からデータ(606)、デジタル署名(608)、作成責任元の証明書C(610)を取り出し(400)、プロセス402で生成した共通鍵(632)を使って暗号化し(404)、このプロセス406によって、暗号化データ622を生成する。次に、データ配送要求者が配送代理人を認証できるような電子封筒616を作成する。まず、402で生成した共通鍵632を、データ配送代理者の秘密鍵B(630)で暗号化(408)し、その成果物と、配送代理者の証明書B(618)をデータ配送要求者の公開鍵Bで暗号化(410)する。この一連の電子封筒生成プロセス(412)により、図6の604部分が生成される。最後に、406、412部分をデータ配送要求者に配送する。

【0042】最後に、図5を用いて、図6の624にあたる、データ配送要求者の復号化、相手認証、ならびにデータ出所認証プロセスを説明する。

【0043】まず、データ配送代理人から受け取った、暗号化データ622と電子封筒616のうち、電子封筒616を、データ配送要求者の秘密鍵Bで復号し、暗号化共通鍵(620)と、配送代理者の証明書B(618)を取り出す(500)。次に、データ配送要求者の証明書Bを用いて、配送された証明書(618)が本物かどうかを検証する(502)。検証できたら、証明書内の公開鍵B(630)を取り出し(504)、506で、暗号化された共通鍵632を復号する。この、502、504、506のプロセス508により、配送要求者は配送代理人を認証することができる。次に、取り出した共通鍵632を用いて暗号化データ622を復号し、データ606、デジタル署名608、作成責任元の証明書C(610)を取り出す(510)。データの出所認証をするために、まず、取り出した作成責任者の証明書C(610)を、同じ証明書発行局で発行された、データ配送要求者の証明書Cを用いて、配送された証明書が本物かどうかを検証する(512)。本物だと確認できたら、証明書(610)から作成責任元の公開鍵C(628)を取り出し(514)、その鍵(628)でデジタル署名(608)を復号し、ハッシュ値を取り出す(516)。ここまでのプロセス512、514、516により、データ出所認証がなされたことになる。最後に、新たに、データのハッシュ値を計算し(518)、516で取り出されたハッシュ値と突き合わせることで、改竄されていないかを確かめられる。

【0044】上述の実施の形態において、3つの証明書発行局を利用した場合を例にとったが、1つの証明書発行局が3者を認証する様な形を取ってもいい。また、公開鍵と秘密鍵のペアは各者1つずつでよく、この公開鍵を各証明書発行局に認証してもらい、証明書を発行してもらう形式でもよい。

# 【0045】

【発明の効果】以上に述べたように、本発明によれば、通信コスト低減のためにデータの作成責任者とデータ配送要求者の間にデータ配送代理人を設置し、データを格納させておいても、データ配送要求者はデータの出所認証を安全に行うことができる。

## 【図面の簡単な説明】

【図1】本発明に関わる、配送代理人を介したデータ配送のシステムブロック図である。

【図2】本発明に関わる、作成責任元でのデータ暗号化プロセスブロック図である。

【図3】本発明に関わる、データ配送代理人でのデータ復号、相手認証、データ格納プロセスブロック図である。

【図4】本発明に関わる、データ配送代理人のデータ暗

号化プロセスブロック図である。

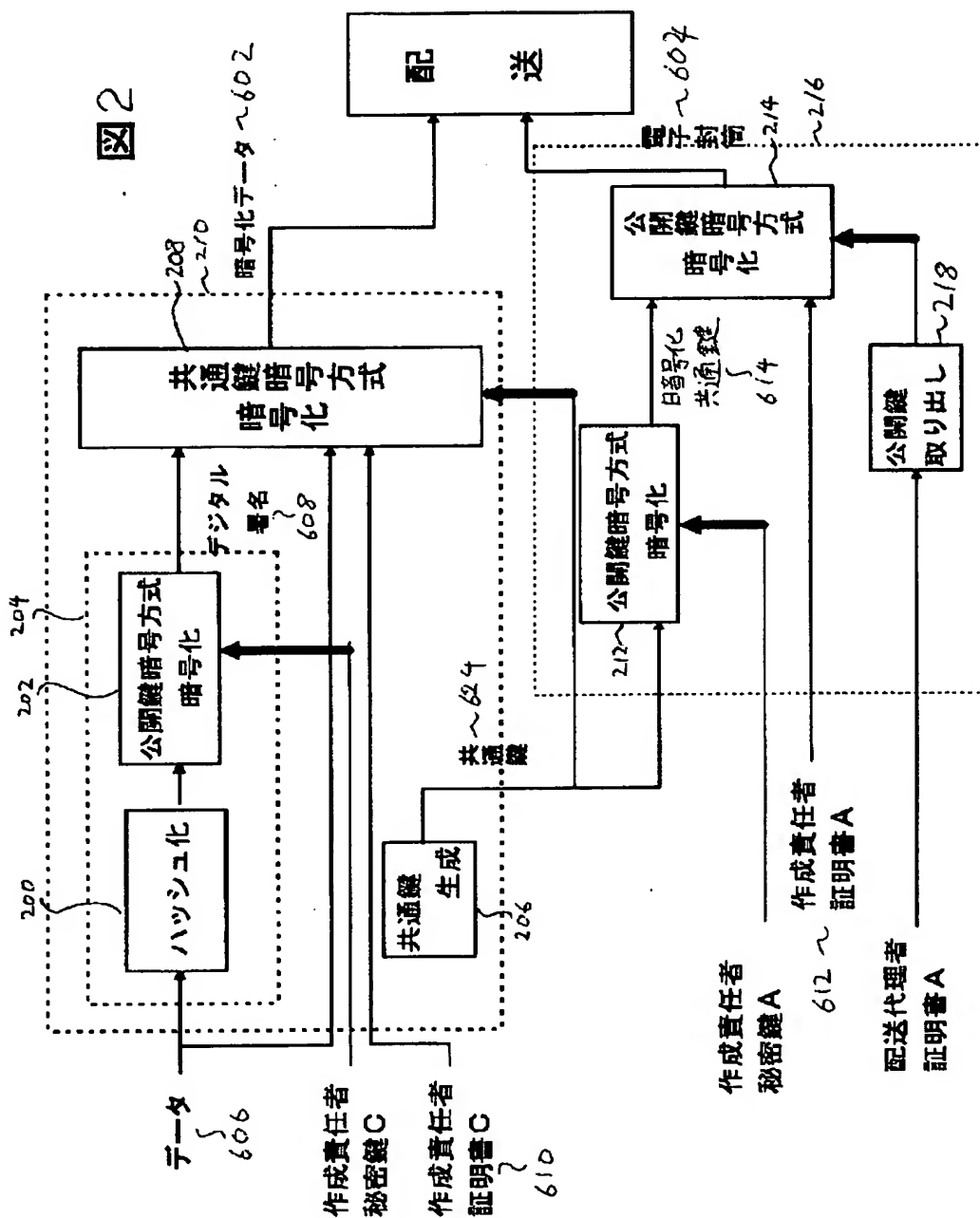
【図5】本発明に関わる、データ配送要求者のデータ復号、配送元認証、データ出所認証プロセスブロック図である。

【図6】本発明に関わる、配送代理人を介したデータ配送における出所認証プロセスの概要図である。

\* 【符号の説明】

100…データ作成責任者側配送サーバ、120…データ配送代理人側配送サーバ/クライアント、140…データ配送要求者側配送クライアント、602…暗号化データ、604…電子封筒。

【図2】



【図 1】

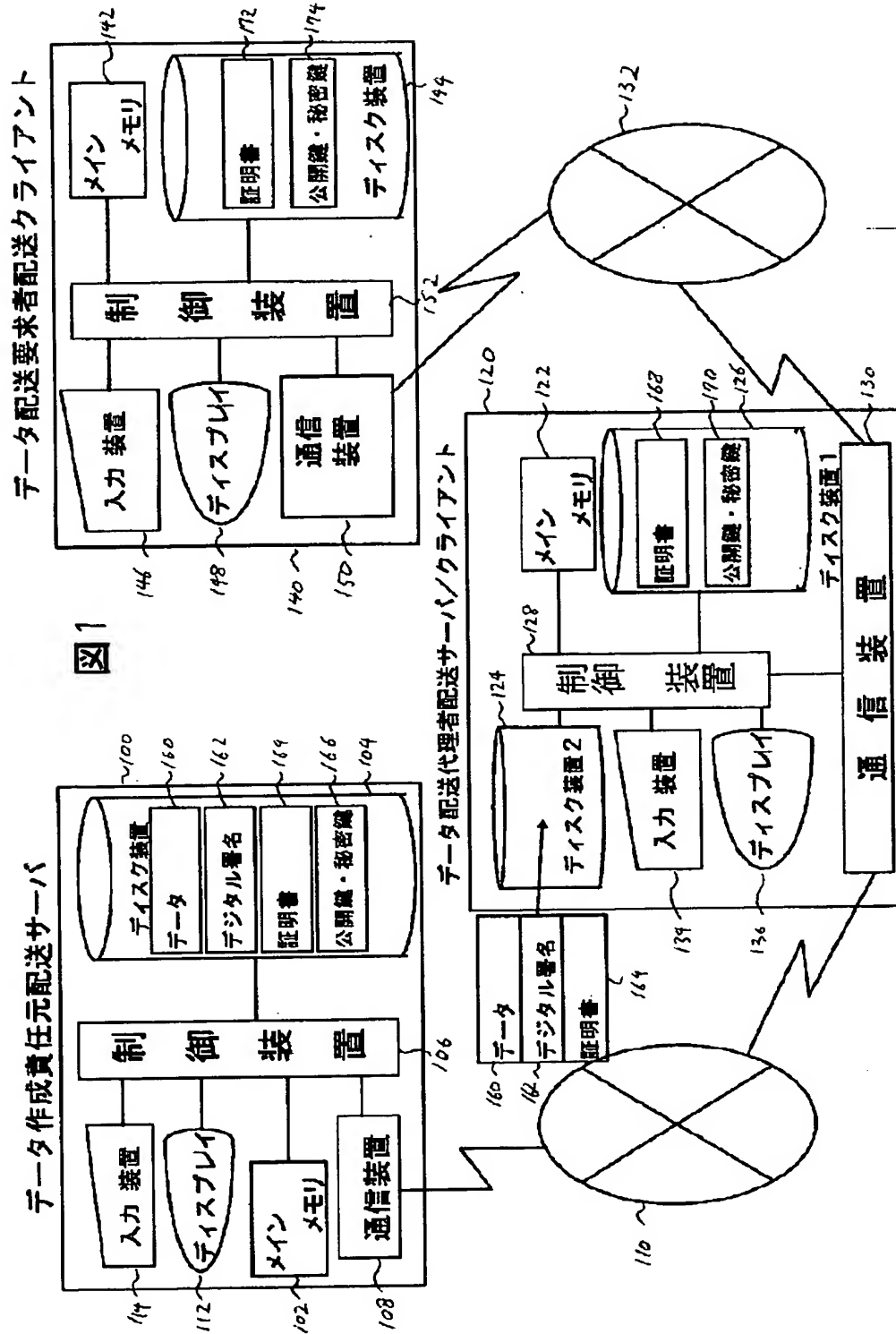




図3

データ作成責任元

データ

デジタル署名

作成 (628)

署名 (629, 619, 609)

データ配送代理者

データ

デジタル署名

保存 (626, 612)

相手 (データ作成責任元) 認証 (614, 604)

データ配送要求者

データ

デジタル署名

出所 (データ作成責任元) 認証 (624, 622, 610, 628)

相手 (データ配送代理人) 認証 (632, 630, 618)

図 6

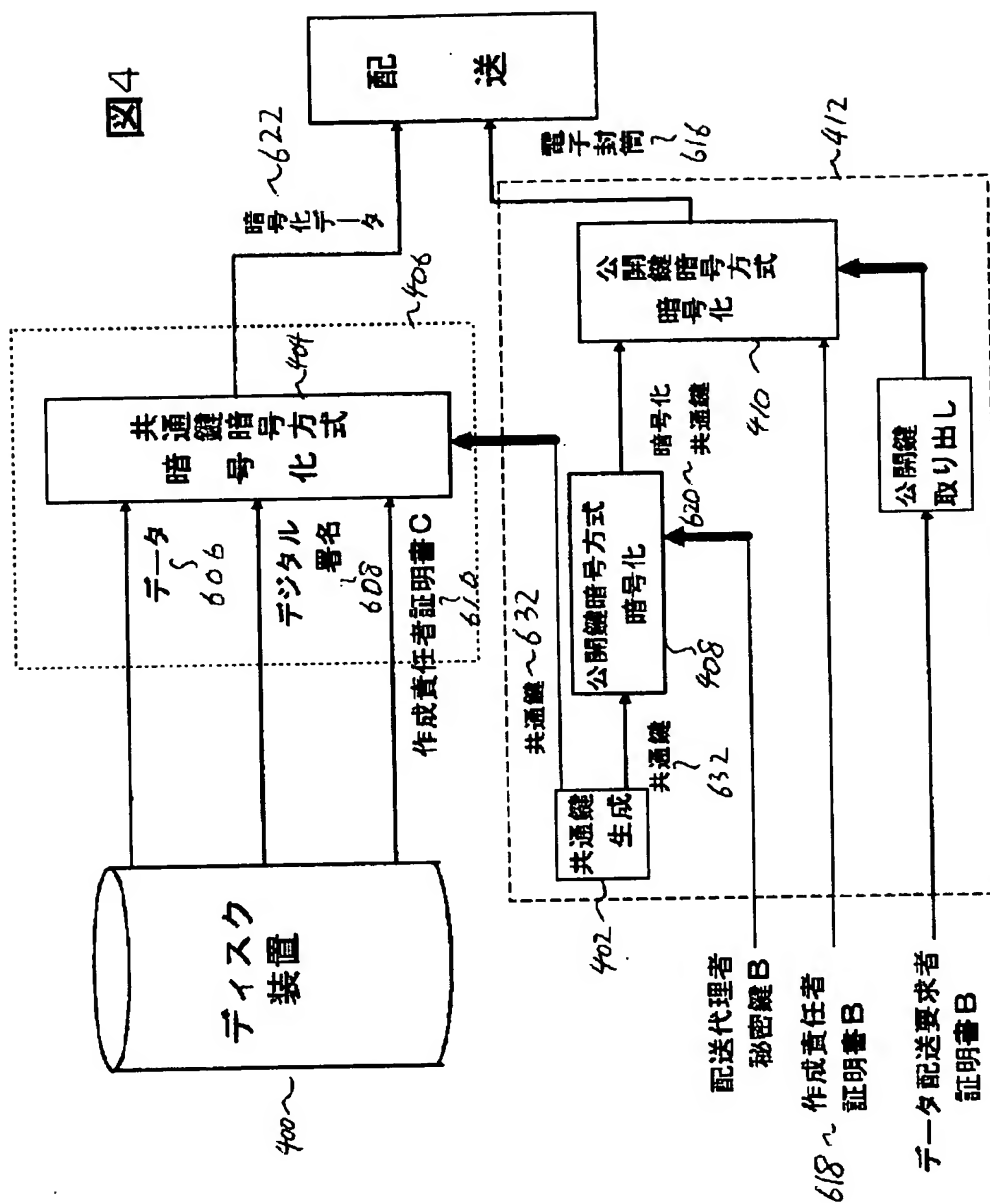


図5

図5は、公開鍵暗号方式を用いたデータ送受信のフローを示している。送信要求者（618）は、配送要求者（616）から電子封筒（500）を受け取り、公開鍵暗号方式復号化（620）を行う。この過程で、配送要求者（616）は送信要求者（618）に公開鍵（502）を提供している。復号化されたデータ（622）は、デジタル署名（608）と共通鍵暗号方式復号化（632）の両方に送られる。デジタル署名（608）は、作成責任元証明書C（606）とデータ（606）を用いて行われ、ハッシュ化（518）と突き合わせチェック（526）の結果（514）を出力する。共通鍵暗号方式復号化（632）は、デジタル署名（608）から提供された共通鍵（506）を用いて行われ、データ（622）を復号化する。最終的に、ハッシュ化（518）と突き合わせチェック（526）の結果（514）が、証明書の認証（512）と組み合わされて、最終的なデータ（516）として出力される。

3 3 0  
6 7 5 A  
6 7 5 B